

Available online at www.sciencedirect.com

Theoretical Computer Science 359 (2006) 176–187

Theoretical
Computer Sciencewww.elsevier.com/locate/tcs

A note on dimensions of polynomial size circuits[☆]

Xiaoyang Gu

Department of Computer Science, Iowa State University, Ames, IA 50011, USA

Received 16 May 2005; received in revised form 8 February 2006; accepted 16 February 2006

Communicated by A. Razborov

Abstract

In this paper, we use resource-bounded dimension theory to investigate polynomial size circuits. We show that for every $i \geq 0$, $P/poly$ has i th-order scaled p_3 -strong dimension 0. We also show that $P/poly^{i.o.}$ has p_3 -dimension $\frac{1}{2}$ and p_3 -strong dimension 1. Our results improve previous measure results of Lutz [Almost everywhere high nonuniform complexity, J. Comput. Syst. Sci. 44(2) (1992) 220–258] and dimension results of Hitchcock and Vinodchandran [Dimension, entropy rates, and compression, in: Proc. 19th IEEE Conf. Computational Complexity, 2004, pp. 174–183, J. Comput. Syst. Sci., to appear]. Additionally, we establish a Supergale Dilation Theorem, which extends the martingale dilation technique introduced implicitly by Ambos-Spies, Terwijn, and Zheng [Resource bounded randomness and weakly complete problems, Theoret. Comput. Sci. 172(1–2) (1997) 195–207] and made explicit by Juedes and Lutz [Weak completeness in E and E_2 , Theoret. Comput. Sci. 143(1) (1995) 149–158].

© 2006 Elsevier B.V. All rights reserved.

Keywords: Resource-bounded dimension; Resource-bounded measures; Circuit complexity

1. Introduction

Circuit-size complexity is one of the most investigated topics in computer science. In particular, much effort has been centered on the relationship between polynomial size circuits and uniform complexity classes. Since the 1970s, it has been known that $SPACE \not\subseteq P/poly^{i.o.}$ [15,14,9,16], i.e., that there exists a language in $SPACE$ that does not have polynomial size circuits, even on only infinitely many lengths.

Lutz invented resource-bounded measure [11] as a powerful tool to examine the quantitative structure within complexity classes and obtained the *quantitative* separation result

$$\mu(P/poly^{i.o.}|SPACE) = 0,$$

which means that it is *typical* for a language in $SPACE$ not to have polynomial size circuits even on only infinitely many lengths. (Precise definitions of this and other notations used in this introduction appear in Sections 2 and 3.) In the same paper, Lutz showed that for all $c > 0$,

$$\mu(SIZE^{i.o.}(n^c)|EXP) = \mu_{p_2}(SIZE^{i.o.}(n^c)) = 0 \quad (1.1)$$

[☆] This research was supported in part by a faculty startup grant of Pavan Aduri and National Science Foundation Grants 9988483 and 0344187.

E-mail address: xiaoyang@cs.iastate.edu

and

$$\mu(\text{P/poly}^{i.o.}|E_3) = \mu_{p_3}(\text{P/poly}^{i.o.}) = 0, \quad (1.2)$$

where $E_3 = \text{DTIME}(2^{2^{\text{poly log } n}})$.

Measure theory does not distinguish among measure 0 sets. In classical analysis, Hausdorff dimension [5] and packing dimension [18,17] serve as refined measurements that complement this limitation of measure. In computational complexity, Lutz et al. effectivized them as the resource-bounded dimension and strong dimension to examine the structure inside resource-bounded measure 0 sets [12,4]. Very soon after the effectivization, Hitchcock, Lutz, and Mayordomo [6] further generalized these dimensions to scaled dimensions to reveal subtle relationships that cannot be addressed without scaling [6]. At the same time, resource-bounded dimension and strong dimension for individual sequences were defined to measure the “level of randomness” for individual sequences [13].

Hitchcock and Vinodchandran [7] recently extended Lutz’s measure results (1.1) and (1.2) with dimension measurements of P/poly. They proved that, for all $c > 0$,

$$\dim(\text{SIZE}(n^c)|\text{EXP}) = \dim_{p_2}(\text{SIZE}(n^c)) = 0 \quad (1.3)$$

and

$$\dim(\text{P/poly}|E_3) = \dim_{p_3}(\text{P/poly}) = 0. \quad (1.4)$$

Recent results by Allender, Buhrman, Koucký, Melkebeek, and Ronneburger [1,2] regarding time-bounded Kolmogorov complexity KT and circuit size complexity of strings enable us to measure the class of polynomial size circuits even more precisely. In Section 4, we use these results to prove our main results, namely, that

$$\dim(\text{SIZE}^{i.o.}(n^c)|\text{EXP}) = \dim_{p_2}(\text{SIZE}^{i.o.}(n^c)) = \frac{1}{2} \quad (1.5)$$

and

$$\dim(\text{P/poly}^{i.o.}|E_3) = \dim_{p_3}(\text{P/poly}^{i.o.}) = \frac{1}{2}. \quad (1.6)$$

Note that (1.5) and (1.6) strengthen (1.1) and (1.2), respectively. They also show that (1.3) and (1.4) cannot be extended to the corresponding i.o.-classes.

Additionally, we prove the strong dimension result

$$\text{Dim}(\text{P/poly}^{i.o.}|E_3) = \text{Dim}_{p_3}(\text{P/poly}^{i.o.}) = 1. \quad (1.7)$$

In order to prove the lower bound on the dimension and strong dimension of P/poly^{i.o.}, we establish a Supergale Dilation Theorem, which extends to dimension theory the measure theoretic martingale dilation technique introduced by Ambos-Spies, Terwijn, and Zheng implicitly in [3] and made explicit by Juedes and Lutz [8].

We also improve Hitchcock and Vinodchandran’s recent results (1.3) and (1.4) from dimension to scaled strong dimension by showing that, for all $c > 0$ and all $i \in \mathbb{N}$,

$$\text{Dim}^{(i)}(\text{SIZE}(n^c)|E_2) = \text{Dim}_{p_2}^{(i)}(\text{SIZE}(n^c)) = 0 \quad (1.8)$$

and

$$\text{Dim}^{(i)}(\text{P/poly}|E_3) = \text{Dim}_{p_3}^{(i)}(\text{P/poly}) = 0. \quad (1.9)$$

Section 2 contains preliminaries. Section 3 is a review of some concepts and properties of resource-bounded measures and dimensions. Section 4 presents our results.

2. Preliminaries

In this paper, *languages* are sets of finite binary strings, i.e., subsets of $\{0, 1\}^*$. The empty string is denoted by λ . The length of a string w is $|w|$ and, in particular, $|\lambda| = 0$. We fix a standard enumeration of all strings as $s_0 = \lambda$, $s_1 = 0$,

$s_2 = 1, s_3 = 00$, etc. \mathbf{C} is *Cantor space*, i.e., $\{0, 1\}^\infty$. $\llbracket \cdot \rrbracket$ is the boolean evaluation function. For a language A , we also identify it with its characteristic sequence $\chi_A \in \mathbf{C}$ such that $\chi_A = \llbracket s_0 \in A \rrbracket \llbracket s_1 \in A \rrbracket \llbracket s_2 \in A \rrbracket \cdots$. We use A for χ_A in this paper. So \mathbf{C} is the set of all languages. For integers $0 \leq i, j < |w|$, $w[i..j] = w[i]w[i+1] \cdots w[j]$ and λ if $j < i$. We use the same convention to identify a finite consecutive part of a sequence also. If string x is prefix of string y , we write $x \sqsubseteq y$. If a string w is a prefix of a sequence S , we write $w \sqsubseteq S$. For any language A , $A^n = A \cap \{0, 1\}^n$. For any class $\mathcal{C} \subseteq \mathbf{C}$, $\mathcal{C}^{i.o.} = \{A \mid (\exists L \in \mathcal{C})(\exists^\infty n)A^n = L^n\}$.

Regarding circuit-size complexity, $\text{SIZE}(f(n)) = \{A \in \mathbf{C} \mid (\forall^\infty n)CS_A(n) \leq f(n)\}$, where $CS_A(n)$ is the number of wires in the smallest n -input Boolean circuit that decides A^n . For $x \in \{0, 1\}^*$, if $|x| = 2^k$ for some $k \in \mathbb{N}$, then define $\text{SIZE}(x)$ as the size of the smallest k -input circuit whose truth table is x . $\text{P/poly} = \bigcup_{c \in \mathbb{N}} \text{SIZE}(n^c)$.

Let s be a time-constructible function. $\text{DTIME}(s)$ is the class of languages decidable in time $O(s)$ by deterministic Turing machines and $\text{DTIMEF}(s)$ is the class of functions computable in time $O(s)$ by deterministic Turing transducers. $\text{DSPACE}(s)$ and $\text{DSPACEF}(s)$ are defined similarly. Δ represents a function class that serves as a resource bound. In this paper, Δ may be one of the following: $\text{pspace} = \text{DSPACEF}(n^{O(1)})$, $p_2 = \text{DTIMEF}(2^{(\log n)^{O(1)}}) = \text{DTIMEF}(n^{(\log n)^{O(1)}})$, and $p_3 = \text{DTIMEF}(2^{2^{(\log \log n)^{O(1)}}})$. Lutz defined resource-bounded constructors [10–12] that generate complexity classes. For a resource bound Δ , the corresponding class is denoted as $R(\Delta)$. The correspondences between resource bounds and complexity classes that we use in this paper are $R(p_2) = E_2 = \text{EXP} = \text{DTIME}(2^{n^{O(1)}})$, $R(p_3) = E_3 = \text{DTIME}(2^{2^{(\log n)^{O(1)}}})$, and $R(\text{pspace}) = \text{ESPACE} = \text{DSPACE}(2^{O(n)})$.

3. Measures and dimensions

In this section, we summarize some concepts and theorems about measures and dimensions that we will use in the development of our results.

Definition. For $s \in [0, \infty)$, an s -supergale is a function $d : \{0, 1\}^* \rightarrow [0, \infty)$ such that for all $w \in \{0, 1\}^*$

$$2^s d(w) \geq d(w0) + d(w1). \quad (3.1)$$

A *supermartingale* is a 1-supergale and a *martingale* is a 1-supergale with equality in (3.1). The *success set* of a s -supergale d is

$$S^\infty[d] = \left\{ S \in \mathbf{C} \mid \limsup_{n \rightarrow \infty} d(S[0..n-1]) = \infty \right\}.$$

We say that d *succeeds* on $S \in \mathbf{C}$ if $S \in S^\infty[d]$. The *strong success set* of d is

$$S_{\text{str}}^\infty[d] = \left\{ S \in \mathbf{C} \mid \liminf_{n \rightarrow \infty} d(S[0..n-1]) = \infty \right\}.$$

We say that d *succeeds strongly* on $S \in \mathbf{C}$ if $S \in S_{\text{str}}^\infty[d]$.

Resource-bounded measures and dimensions are defined by imposing resource bounds on the computation of supergales.

Definition. A function $f : \{0, 1\}^* \rightarrow \mathbb{R}$ is Δ -computable if there is a function $\hat{f} : \{0, 1\}^* \times \mathbb{N} \rightarrow \mathbb{Q}$ such that $\hat{f} \in \Delta$ and for all $w \in \{0, 1\}^*$ and $r \in \mathbb{N}$, $|\hat{f}(w, r) - d(w)| \leq 2^{-r}$, where r is represented in unary.

Definition (Lutz [11]). Let $X \subseteq \mathbf{C}$. X has Δ -measure 0, and we write $\mu_\Delta(X) = 0$ if there exists a Δ -computable supermartingale d such that $X \subseteq S^\infty[d]$. X has Δ -measure 1 if X^c has Δ -measure 0. X has *measure* 0 in $R(\Delta)$ if $\mu_\Delta(X \cap R(\Delta)) = 0$. X has *measure* 1 in $R(\Delta)$ if $\mu_\Delta(X^c \cap R(\Delta)) = 0$.

Definition (Lutz [12], Athreya, Hitchcock, Lutz, and Mayordomo [4]). Let $X \subseteq \mathbf{C}$. The Δ -dimension of X is

$$\dim_{\Delta}(X) = \inf\{s \in [0, \infty) \mid X \subseteq S^{\infty}[d] \text{ for some } \Delta\text{-computable } s\text{-supergale } d\}.$$

The Δ -strong dimension of X , denoted $\text{Dim}_{\Delta}(X)$, is defined similarly with respect to strong success. The dimension of X in $R(\Delta)$ is $\dim(X|R(\Delta)) = \dim_{\Delta}(X \cap R(\Delta))$. The strong dimension of X in $R(\Delta)$ is $\text{Dim}(X|R(\Delta)) = \text{Dim}_{\Delta}(X \cap R(\Delta))$.

When Δ is the set of all functions (with no computational restriction), the above definitions of dimension and strong dimension give us the classical Hausdorff dimension $\dim_{\mathbf{H}}$ and packing dimension $\text{dim}_{\mathbf{p}}$, respectively.

Observation 3.1 (Lutz [12], Athreya, Hitchcock, Lutz, and Mayordomo [4]). 1. For all $X \subseteq \mathbf{C}$ and all resource bounds Δ , if $\dim_{\Delta}(X) < 1$ then $\mu_{\Delta}(X) = 0$.

2. For all $X \subseteq \mathbf{C}$ and all resource bounds Δ , $\dim_{\Delta}(X) \leq \text{Dim}_{\Delta}(X)$.

3. For all $X \subseteq Y$ and all resource bounds Δ , $\dim_{\Delta}(X) \leq \dim_{\Delta}(Y)$.

4. Let Δ, Δ' be resource bounds such that $\Delta \subseteq \Delta'$. Then for all $X \subseteq \mathbf{C}$, $\dim_{\Delta'}(X) \leq \dim_{\Delta}(X)$, and $\text{Dim}_{\Delta'}(X) \leq \text{Dim}_{\Delta}(X)$.

In contrast to classical measure and dimension theory, when resource bounds are enforced on the computation of supergales, there are individual sequences that are not in the success set of any supergales. Therefore, dimensions of individual sequences can now be defined.

Definition. Let $S \in \mathbf{C}$ be an infinite binary sequence. The Δ -dimension of S is $\dim_{\Delta}(S) = \dim_{\Delta}(\{S\})$. The Δ -strong dimension of S is $\text{Dim}_{\Delta}(S) = \text{Dim}_{\Delta}(\{S\})$.

Hitchcock, Lutz, and Mayordomo also introduced a theory of resource-bounded scaled dimension that has more distinguishing power for some problems in complexity theory.

Definition (Hitchcock, Lutz, and Mayordomo [6]). A scale is a continuous function $g : H \times [0, \infty) \rightarrow \mathbb{R}$ such that $H = (a, \infty)$ for some $a \in \mathbb{R} \cup \{-\infty\}$; $g(m, 1) = m$ for all $m \in H$; $g(m, 0) = g(m', 0) \geq 0$ for all $m, m' \in H$; for every sufficiently large $m \in H$, the function $s \mapsto g(m, s)$ is nonnegative and strictly increasing; and for all $s' > s \geq 0$, $\lim_{m \rightarrow \infty} [g(m, s') - g(m, s)] = \infty$.

Definition (Hitchcock, Lutz, and Mayordomo [6]). Let $g : H \times [0, \infty) \rightarrow \mathbb{R}$ be a scale, and let $s \in [0, \infty)$. A g -scaled s -supergale ($s^{(g)}$ -supergale) is a function $d : \{0, 1\}^* \rightarrow [0, \infty)$ such that for all $w \in \{0, 1\}^*$ with $|w| \in H$,

$$d(w) \geq 2^{-\Delta g(|w|, s)} [d(w0) + d(w1)], \quad (3.2)$$

where $\Delta g(m, s) = g(m+1, s) - g(m, s)$.

The definitions for scaled dimensions are identical to those of regular dimensions except that they use scaled supergales. In corresponding notations, we use superscript (g) to indicate the scale as in $\dim_{\Delta}^{(g)}(\cdot)$, $\text{Dim}_{\Delta}^{(g)}(\cdot)$.

In this paper, we use the scales g_i , for $i \geq 0$, defined as follows.

Definition (Hitchcock, Lutz, and Mayordomo [6]). Let $g : H \times [0, \infty) \rightarrow \mathbb{R}$ be a scale.

1. The first rescaling of g is the scale $g^{\#} : H^{\#} \times [0, \infty) \rightarrow \mathbb{R}$ defined by

$$\begin{aligned} H^{\#} &= \{2^m \mid m \in H\}, \\ g^{\#}(m, s) &= 2^{g(\log m, s)}. \end{aligned}$$

2. For each $i \in \mathbb{N}$, $a_0 = -\infty$, $a_{i+1} = 2^{a_i}$.

3. For each $i \in \mathbb{N}$, the i th scale $g_i : (a_i, \infty) \times [0, \infty) \rightarrow \mathbb{R}$ is defined such that

(a) $g_0(m, s) = sm$.

(b) For $i \geq 0$, $g_{i+1} = g_i^{\#}$.

When these scales are used, we use superscript (i) instead of (g_i) . We call $\dim^{(i)}$ and $\text{Dim}^{(i)}$ the i th-order scaled dimension and the i th-order scaled strong dimension, respectively. Resource-bounded zeroth scaled dimensions and strong dimensions coincide with the regular dimensions and strong dimensions. With the scales defined above, it was shown that the scaled dimensions exhibit the following monotonicity with respect to the order of the scale.

Theorem 3.2 (Hitchcock, Lutz, and Mayordomo [6]). *Let $i \in \mathbb{N}$ and $X \subseteq \mathbf{C}$. If $\dim_{\Delta}^{(i+1)}(X) < 1$, then $\dim_{\Delta}^{(i)}(X) = 0$.*

In this paper, we also use the Measure Conservation Theorem.

Theorem 3.3 (Lutz [11]). *$R(\Delta)$ does not have measure 0 in $R(\Delta)$.*

4. Polynomial size circuits

Our starting point is the following theorem regarding polynomial size circuits.

Theorem 4.1 (Lutz [11]). *For all $c > 0$,*

$$\mu(\text{SIZE}^{\text{i.o.}}(n^c) | \text{EXP}) = \mu_{p_2}(\text{SIZE}^{\text{i.o.}}(n^c)) = 0$$

and

$$\mu(\text{P/poly}^{\text{i.o.}} | \text{E}_3) = \mu_{p_3}(\text{P/poly}^{\text{i.o.}}) = 0.$$

This result was recently improved to dimension as follows.

Theorem 4.2 (Hitchcock and Vinodchandran [7]). *For all $c \geq 1$,*

$$\dim(\text{SIZE}(n^c) | \text{EXP}) = \dim_{p_2}(\text{SIZE}(n^c)) = 0$$

and

$$\dim(\text{P/poly} | \text{E}_3) = \dim_{p_3}(\text{P/poly}) = 0.$$

In this section, we use the relationship between time-bounded Kolmogorov complexity and circuit complexity to give a more thorough analysis of the dimensions of polynomial size circuits.

Definition (Allender [1]). Let U be a universal Turing machine. Define $\text{KT}(x)$ to be

$$\min\{|p| + t \mid \text{for all } i \leq |x|, U(p, i) = x_i \text{ in at most } t \text{ steps}\}.$$

Theorem 4.3 (Allender [1], Allender et al. [2]). $\text{SIZE}(x) = O((\text{KT}(x))^4)$, and $\text{KT}(x) = O((\text{SIZE}(x))^2 \cdot (\log(\text{SIZE}(x))^2 + \log |x|))$.

Lemma 4.4. *Let $A \subseteq \{0, 1\}^*$.*

1. *$A \in \text{P/poly}^{\text{i.o.}}$ if and only if for some integer $c \in \mathbb{N}$, $\text{KT}(A[2^n - 1..2^{n+1} - 2]) \leq n^c$ for infinitely many $n \in \mathbb{N}$.*
2. *$A \in \text{P/poly}$ if and only if for some integer $c \in \mathbb{N}$, $\text{KT}(A[2^n - 1..2^{n+1} - 2]) \leq n^c$ for all but finitely many $n \in \mathbb{N}$.*

Proof. Both follow from Theorem 4.3. \square

Using this lemma, we first establish the following two theorems for individual languages concerning $\text{P/poly}^{\text{i.o.}}$ and P/poly .

Theorem 4.5. *Let $A \subseteq \{0, 1\}^*$ be a language such that $\dim_{p_2}(A) > \frac{1}{2}$. Then $A \notin \text{P/poly}^{\text{i.o.}}$.*

Proof. We prove the contrapositive. Assume that $A \in \text{P/poly}^{i.o.}$. Then by Lemma 4.4, $\text{KT}(A[2^n - 1..2^{n+1} - 2]) < n^c$ for infinitely many n and some fixed constant c . It suffices to show that $\dim_{p_2}(A) \leq \frac{1}{2}$.

Let $r > \frac{1}{2}$ be a polynomial-time computable real number. It suffices to show that there exists a p_2 -computable r -supergale d that succeeds on A .

For $i \geq 1$ and $w \in \{0, 1\}^*$, let

$$C_i = \{x \in \{0, 1\}^{2^i} \mid \text{KT}(x) < i^c\},$$

$$C_i^w = \{x \in C_i \mid w[2^i - 1..|w| - 1] \sqsubseteq x\},$$

and let d_i be such that

$$d_i(w) = \begin{cases} 2^{(r-1)|w|} & \text{if } |w| < 2^i, \\ d_i(w[0..2^i - 2])2^{r(|w| - (2^i - 1))} \frac{|C_i^w|}{|C_i|} & \text{if } 2^i \leq |w| \leq 2^{i+1} - 1, \\ 2^{(r-1)(|w| - (2^{i+1} - 1))} d_i(w[0..2^{i+1} - 2]) & \text{if } |w| > 2^{i+1} - 1. \end{cases}$$

We compute d_i by simulating the universal Turing machine U to enumerate C_i by cycling all programs of length up to i^c and all bit indices less than or equal to 2^i within running time less than i^c . For every such program, a valid simulation generates 2^i bits and by concatenating them, we get an output string of length 2^i in C_i . During the enumeration, d_i counts the number of strings in C_i and in C_i^w to get $|C_i|$ and $|C_i^w|$. Note that $|C_i| \leq 2^{i^c}$.

Let $d = \sum_{i=1}^{\infty} (1/2^i) d_i$. It is easy to verify that d is a p_2 -computable r -supergale.

For any $n \geq 1$ such that $\text{KT}(A[2^n - 1..2^{n+1} - 2]) < n^c$, we have

$$\begin{aligned} d(A[0..2^{n+1} - 2]) &\geq \frac{1}{2^n} d_n(A[0..2^{n+1} - 2]) \\ &\geq \frac{1}{2^n} 2^{(r-1)(2^n - 1)} 2^{r2^n} \frac{|C_n^{A[0..2^{n+1} - 2]}|}{|C_n|} \\ &\geq \frac{2^{(2r-1)2^n - r + 1}}{2^n \cdot 2^{n^c}}. \end{aligned}$$

Since $r > \frac{1}{2}$ and $\text{KT}(A[2^n - 1..2^{n+1} - 2]) < n^c$ for infinitely many n , it follows that the value that the r -supergale d can obtain along A is unbounded, and thus $\dim_{p_2}(A) \leq r$. Since polynomial-time computable real numbers are dense in \mathbb{R} , it follows that $\dim_{p_2}(A) \leq \frac{1}{2}$. \square

Corollary 4.6. For $c > 0$,

$$\dim(\text{SIZE}^{i.o.}(n^c) | \text{EXP}) \leq \frac{1}{2} \quad \text{and} \quad \dim_{p_2}(\text{SIZE}^{i.o.}(n^c)) \leq \frac{1}{2}$$

and

$$\dim(\text{P/poly}^{i.o.} | \text{E}_3) \leq \frac{1}{2} \quad \text{and} \quad \dim_{p_3}(\text{P/poly}^{i.o.}) \leq \frac{1}{2}.$$

Proof. By Theorem 4.5 and standard universal simulation techniques, $\text{SIZE}^{i.o.}(n^c)$ is a p_2 -union of sets of p_2 -dimension at most $\frac{1}{2}$, and $\text{P/poly}^{i.o.}$ is a p_3 -union of sets of p_2 -dimension (hence p_3 -dimension) at most $\frac{1}{2}$. The corollary then follows by the effective stability of resource-bounded dimension [12, Lemma 4.11]. \square

By changing the simulation in the proof of Theorem 4.5 from cycling programs of length exactly i to cycling programs of length at most i , we can establish an analogous result regarding P/poly , but now with strong dimension.

Theorem 4.7. Let $A \subseteq \{0, 1\}^*$ be a language such that $\text{Dim}_{p_2}(A) > 0$. Then $A \notin \text{P/poly}$.

Proof. We prove the contrapositive. Assume that $A \in \text{P/poly}$. Then by Lemma 4.4, $\text{KT}(A[2^n - 1..2^{n+1} - 2]) < n^c$ for all but finitely many $n \in \mathbb{N}$ and some fixed constant c . It suffices to show that $\text{Dim}_{p_2}(A) = 0$.

Let $r > 0$ be a polynomial-time computable real number. It suffices to show that there exists a p_2 -computable r -supergale d that succeeds on A .

For $i \geq 1$ and $w \in \{0, 1\}^*$, let

$$C_{\leq i} = \{x \in \{0, 1\}^{2^{i+1}-1} \mid \text{KT}(x[2^k - 1..2^{k+1} - 2]) < k^c, 0 < k \leq i\},$$

$$C_{\leq i}^w = \{x \in C_{\leq i} \mid w \sqsubseteq x\},$$

and let d_i be such that

$$d_i(w) = \begin{cases} 2^{r|w|} \frac{|C_{\leq i}^w|}{|C_{\leq i}|} & \text{if } |w| \leq 2^{i+1} - 1, \\ 2^{(r-1)(|w|-(2^{i+1}-1))} d_i(w[0..2^{i+1}-2]) & \text{if } |w| > 2^{i+1} - 1. \end{cases}$$

We compute d_i by simulating the universal Turing machine U to enumerate $C_{\leq i}$ by cycling all programs of length at most k^c and all bit indices less than or equal to 2^k within running time less than k^c for $k = 0, 1, \dots, i$ in a depth first fashion. For every such k and a particular program, a valid simulation generates 2^k bits and by concatenating them, we get an output string of length 2^k . By concatenating the outputs for k from 0 to i , we get a string of length $2^{i+1} - 1$ in $C_{\leq i}$. $|C_{\leq i}|$ and $|C_{\leq i}^w|$ are obtained, respectively, by counting the number of strings in $C_{\leq i}$ and the number of those strings with w as a prefix. Note that $|C_{\leq i}| \leq 2^{i^{c+1}}$.

Let $d = \sum_{i=1}^{\infty} (1/2^i) d_i$. It is easy to verify that d is a p_2 -computable r -supergale.

For any $n > 1$ and $0 < k \leq 2^n$, we have

$$\begin{aligned} d(A[0..2^n - 2 + k]) &\geq \frac{1}{2^n} d_n(A[0..2^n - 2 + k]) \\ &= \frac{1}{2^n} 2^{r(2^n-1+k)} \frac{|C_{\leq n}^{A[0..2^n-2+k]}|}{|C_{\leq n}|} \\ &\geq \frac{1}{2^n} 2^{r(2^n-1+k)} \frac{1}{2^{n^{c+1}}}. \end{aligned}$$

Since $r > 0$ and $k > 0$, it follows that the value that the r -supergale d can obtain along A goes to infinity, i.e.,

$$\liminf_{n \rightarrow \infty} d(A[0..n - 1]) = \infty.$$

So the r -supergale d succeeds strongly on A , and hence the $\text{Dim}_{p_2}(A) \leq r$. By the density of polynomial-time computable real numbers, $\text{Dim}_{p_2}(A) = 0$. \square

Our next theorem shows that scaled dimension can be used to significantly relax the hypothesis of Theorem 4.7. We first give an observation about the transformation between different scaled supergales that simplifies the calculation of scaled dimensions.

Observation 4.8. Let g_1, g_2 be two scales and $s_1, s_2 \in [0, \infty)$. Let $d : \{0, 1\}^* \rightarrow [0, \infty)$ be a g_1 -scaled s_1 -supergale ($s_1^{(g_1)}$ -supergale), i.e.,

$$d(w) \geq 2^{-\Delta_{g_1}(|w|, s_1)} [d(w0) + d(w1)].$$

Then the function $d' : \{0, 1\}^* \rightarrow [0, \infty)$ defined by $d'(w) = d(w) 2^{g_2(|w|, s_2) - g_1(|w|, s_1)}$ is an $s_2^{(g_2)}$ -supergale.

Proof. This observation follows from easy verification of the $s_2^{(g_2)}$ -supergale condition (3.2). \square

Now we use Observation 4.8 to extend Theorem 4.7 to scales of arbitrary nonnegative order.

Theorem 4.9. Let $j \in \mathbb{N}$ and $A \subseteq \{0, 1\}^*$ be a language such that $\text{Dim}_{p_2}^{(j)}(A) > 0$. Then $A \notin \text{P/poly}$.

Proof. We prove the contrapositive. Assume that $A \in \text{P/poly}$. Then by Lemma 4.4, $\text{KT}(A[2^n - 1..2^{n+1} - 2]) < n^c$ for all but finitely many $n \in \mathbb{N}$ and some fixed constant c . It suffices to show that $\text{Dim}_{\text{p}_2}^{(j)}(A) = 0$.

Let $s > 0$ be a polynomial-time computable real number. It suffices to show that there exists a p_2 -computable $s^{(j)}$ -supergale that succeeds on A .

Let $r > 0$ be a polynomial-time computable real number. For all $i \in \mathbb{N}$, let d_i be defined as in the proof of Theorem 4.7 and similarly let $d = \sum_{i=1}^{\infty} (1/2^i)d_i$. It is clear that d is a p_2 -computable r -supergale.

Define d' such that

$$d'(w) = d(w)2^{g_j(|w|,s) - g_0(|w|,r)}.$$

By Observation 4.8, d' is a p_2 -computable $s^{(j)}$ -supergale and

$$\begin{aligned} d'(A[0..2^n - 2 + k]) &\geq \frac{1}{2^n} d_n(A[0..2^n - 2 + k]) \frac{2^{g_j(2^n - 1 + k, s)}}{2^{r(2^n - 1 + k)}} \\ &\geq \frac{1}{2^n} \frac{2^{r(2^n - 1 + k)}}{2^{n^{c+1}}} \frac{2^{g_j(2^n - 1 + k, s)}}{2^{r(2^n - 1 + k)}} \\ &= \frac{2^{g_j(2^n - 1 + k, s)}}{2^n \cdot 2^{n^{c+1}}}. \end{aligned}$$

Since $s > 0$, $c \in \mathbb{N}$, $k > 0$, the growth rate of the function $g_j(2^n - 1 + k, s)$ is higher than that of the function n^{c+1} . It follows that $\liminf_{n \rightarrow \infty} d'(A[0..2^n - 2 + k]) = \infty$, i.e., $\text{Dim}_{\text{p}_2}^{(j)}(A) = 0$. \square

By using Theorems 4.7 and 4.9 together with the same techniques used in the proof of Corollary 4.6, we obtain (1.8) and (1.9) as the following theorem.

Theorem 4.10. For all $c > 0$ and all $i \in \mathbb{N}$,

$$\text{Dim}^{(i)}(\text{SIZE}(n^c) | \text{EXP}) = \text{Dim}_{\text{p}_2}^{(i)}(\text{SIZE}(n^c)) = 0$$

and

$$\text{Dim}^{(i)}(\text{P/poly} | \text{E}_3) = \text{Dim}_{\text{p}_3}^{(i)}(\text{P/poly}) = 0.$$

Jack Lutz suggested that the upper bounds for dimensions in Corollary 4.6 are tight. We prove a general theorem on dimension lower bound of infinitely-often classes, which is then used to show that the inequalities in Corollary 4.6 may be replaced by equalities. In the proof, we will use the supergale dilation technique, which is an extension of the martingale dilation technique introduced by Ambos-Spies, Terwijn, and Zheng implicitly [3] and made explicit by Juedes and Lutz [8]. In the following, we only state and prove the case for nonnegative scales of dimensions and strong dimensions. Both the theorem and the corollary generalize to negative scales.

Definition. Let $f : \{0, 1\}^* \rightarrow \{0, 1\}^*$. We call f a *dilation* if for all $x, y \in \{0, 1\}^*$ with $x \sqsubseteq y$, $f(x) \sqsubseteq f(y)$, and for all x , there exists $x \sqsubseteq x'$ such that $f(x) \sqsubsetneq f(x')$, and $|f(x0)| = |f(x1)| \leq |f(x)| + 1$ for all $x \in \{0, 1\}^*$.

Let f be a dilation. For $A \in \mathbf{C}$, let $f(A) = S \in \mathbf{C}$ such that $f(A[0..n - 1]) \sqsubseteq S$ for all $n \in \mathbb{N}$. We call $f(A)$ the f -dilation of A . For $x \in \{0, 1\}^*$, define the *collision set of f on x* as

$$\text{Col}(f, x) = \{0 \leq n < |x| \mid f(x[0..n - 1]0) = f(x[0..n - 1]1) \neq f(x[0..n - 1])\}.$$

Theorem 4.11 (Supergale dilation theorem). Let $\mathcal{C} \subseteq \mathbf{C}$, Δ be a resource bound, $i, j \in \mathbb{N}$ and $s, s' \in [0, 1]$. Let f be a Δ -computable dilation.

1. If $\dim_{\Delta}^{(i)}(f(\mathcal{C})) < s$ and for every $A \in \mathcal{C}$,

$$g_i(|f(A[0..n - 1])|, s) + |\text{Col}(f, A[0..n - 1])| \leq g_j(n, s') - n + |f(A[0..n - 1])| \quad (4.1)$$

for all but finitely many n , then $\dim_{\Delta}^{(j)}(\mathcal{C}) \leq s'$.

2. If $\dim_{\Delta}^{(i)}(f(\mathcal{C})) < s$ and for every $A \in \mathcal{C}$, (4.1) holds for infinitely many n , then $\dim_{\Delta}^{(j)}(\mathcal{C}) \leq s'$.
 3. If $\dim_{\Delta}^{(i)}(f(\mathcal{C})) < s$ and for every $A \in \mathcal{C}$, (4.1) holds for all but finitely many n , then $\dim_{\Delta}^{(j)}(\mathcal{C}) \leq s'$.

Note that in contrast to [3,8], we are looking at the dilation from a different perspective. In [3,8], the dilation is defined in terms of strings (in languages). In this paper, the dilation is defined in terms of the prefixes of characteristic sequences of languages. It is easy to verify that every dilation that is consistent with [8] can be written in a way that is consistent with the definition in this paper. But the converse is not true.

Proof. We prove 1; the proofs of 2 and 3 are similar. Since $\dim_{\Delta}^{(j)}(\mathcal{C}) \leq 1$, the theorem is true when $s' \geq 1$. Assume $s' < 1$, $\dim_{\Delta}^{(i)}(f(\mathcal{C})) < s$ and (4.1). Then, by Observation 4.8, there exists a Δ -computable supermartingale d such that for every $A \in \mathcal{C}$ and some $\varepsilon > 0$,

$$d(f(A[0..n-1])) \geq 2^{|f(A[0..n-1])| - g_i(|f(A[0..n-1])|, s - \varepsilon)} \quad (4.2)$$

for infinitely many n . Define d' with the following recursion.

$$\begin{cases} d'(\lambda) = d(f(\lambda)), \\ d'(wb) = 2d'(w) \frac{d(f(wb))}{d(f(w0)) + d(f(w1))}. \end{cases}$$

Since f is Δ -computable, it is clear that d' is a Δ -computable martingale. Note that

$$d'(A[0..n-1]) = d(f(A[0..n-1])) \prod_{i=0}^{n-2} \frac{d(f(A[0..i])) \cdot 2}{d(f(A[0..i]0)) + d(f(A[0..i]1))}.$$

Since d is a martingale, for each $i \notin \text{Col}(f, A[0..n-1])$

$$\frac{d(f(A[0..i])) \cdot 2}{d(f(A[0..i]0)) + d(f(A[0..i]1))} = 1$$

and $i \in \text{Col}(f, A[0..n-1])$

$$\frac{d(f(A[0..i])) \cdot 2}{d(f(A[0..i]0)) + d(f(A[0..i]1))} \geq \frac{1}{2}.$$

Therefore,

$$d'(A[0..n-1]) \geq \frac{d(f(A[0..n-1]))}{2^{|\text{Col}(f, A[0..n-1])|}}.$$

Since (4.2) holds for infinitely many n , and (4.1) holds for all but finitely many n , we have that, for infinitely many n ,

$$\begin{aligned} d'(A[0..n-1]) &\geq \frac{2^{|f(A[0..n-1])| - g_i(|f(A[0..n-1])|, s - \varepsilon)}}{2^{g_j(n, s') - n + |f(A[0..n-1])| - g_i(|f(A[0..n-1])|, s)}} \\ &> 2^{n - g_j(n, s')}. \end{aligned}$$

Since $\lim_{n \rightarrow \infty} 2^{n - g_j(n, s')} = \infty$ for $s' < 1$, $\dim_{\Delta}^{(j)}(\mathcal{C}) \leq s'$. \square

Corollary 4.12. Let $\mathcal{C} \subseteq \mathbf{C}$, Δ be a resource bound, $i, j \in \mathbb{N}$ and $s, s' \in [0, 1]$. Let f be a Δ -computable dilation.

1. If $\dim^{(i)}(f(\mathcal{C})|R(\Delta)) < s$ and for every $A \in \mathcal{C}$, (4.1) holds for all but finitely many n , then $\dim^{(j)}(\mathcal{C}|R(\Delta)) \leq s'$.
 2. If $\text{Dim}^{(i)}(f(\mathcal{C})|R(\Delta)) < s$ and for every $A \in \mathcal{C}$, (4.1) holds for infinitely many n , then $\dim^{(j)}(\mathcal{C}|R(\Delta)) \leq s'$.
 3. If $\text{Dim}^{(i)}(f(\mathcal{C})|R(\Delta)) < s$ and for every $A \in \mathcal{C}$, (4.1) holds for all but finitely many n , then $\text{Dim}^{(j)}(\mathcal{C}|R(\Delta)) \leq s'$.

Proof. We prove 1; the proofs of 2 and 3 are similar.

Note that $f(\mathcal{C} \cap R(\Delta)) \subseteq R(\Delta)$ and $f(\mathcal{C} \cap R(\Delta)) \subseteq f(\mathcal{C})$. Therefore, $f(\mathcal{C} \cap R(\Delta)) \subseteq f(\mathcal{C}) \cap R(\Delta)$.

Since $\dim_{\Delta}^{(i)}(f(\mathcal{C}) \cap R(\Delta)) = \dim^{(i)}(f(\mathcal{C})|R(\Delta)) < s$, $\dim_{\Delta}^{(i)}(f(\mathcal{C} \cap R(\Delta))) < s$. Now apply Theorem 4.11 and we have

$$\dim_{\Delta}^{(j)}(\mathcal{C} \cap R(\Delta)) < s',$$

i.e., $\dim^{(j)}(\mathcal{C}|R(\Delta)) \leq s'$. \square

Theorem 4.13. *Let \mathcal{C} be a language class that contains the trivial language \emptyset . Then for all $\Delta \supseteq p$, $\dim(\mathcal{C}^{i.o.}|R(\Delta)) \geq 1/2$ and $\text{Dim}(\mathcal{C}^{i.o.}|R(\Delta)) = 1$.*

Proof. Let $f : \{0, 1\}^* \rightarrow \{0, 1\}^*$ be defined such that for all $x \in \{0, 1\}^*$, $|f(x)| = |x|$ and for all $i < |x|$,

$$f(x)[i] = \begin{cases} 0, & |s_i| = 2^k \text{ for some } k, \\ x[i] & \text{otherwise.} \end{cases}$$

It is clear that f is a p -computable dilation.

By the construction of f , it is easy to see that $f(R(\Delta)) \subseteq \mathcal{C}^{i.o.}$. Also note that $f(R(\Delta)) \subseteq R(\Delta)$.

Let

$$\#n = |\{i < n \mid |s_i| = 2^k \text{ for some } k\}|.$$

Note that for all $n \in \mathbb{N}$ and all $A \in \mathbf{C}$,

$$|\text{Col}(f, A[0..n-1])| = \#n$$

and

$$|f(A[0..n-1])| = n.$$

It is easy to verify that for every $A \in R(\Delta)$,

$$|\text{Col}(f, A[0..n-1])| \leq n/2 + 2\sqrt{n/2}$$

for all but finitely many n and

$$|\text{Col}(f, A[0..n-1])| \leq \sqrt{n}$$

for infinitely many n . Let $\varepsilon > 0$. Now we have that, for all but finitely many n ,

$$\begin{aligned} (1/2 - 2\varepsilon)n + |\text{Col}(f, A[0..n-1])| &\leq n/2 - 2\varepsilon n + n/2 + 2\sqrt{n/2} \\ &= (1 - 2\varepsilon)n + 2\sqrt{n/2} \\ &\leq (1 - \varepsilon)n, \end{aligned}$$

i.e.,

$$g_0(n, 1/2 - 2\varepsilon) + |\text{Col}(f, A[0..n-1])| \leq g_0(n, 1 - \varepsilon) \quad \text{for all but finitely many } n. \quad (4.3)$$

And similarly

$$g_0(n, 1 - 2\varepsilon) + |\text{Col}(f, A[0..n-1])| \leq g_0(n, 1 - \varepsilon) \quad \text{for infinitely many } n. \quad (4.4)$$

Note that $\dim(\mathcal{C}^{i.o.}|R(\Delta)) < \frac{1}{2}$ implies that $\dim_{\Delta}(f(R(\Delta))) = \dim(f(R(\Delta))|R(\Delta)) < \frac{1}{2}$. By Theorem 4.11 and (4.3), $\dim(\mathcal{C}^{i.o.}|R(\Delta)) < \frac{1}{2}$ then implies that $\dim_{\Delta}(R(\Delta)) < 1$, which by Observation 3.1, implies $\mu_{\Delta}(R(\Delta)) = 0$. By the Measure Conservation Theorem, we know that $\mu_{\Delta}(R(\Delta)) = 1$. Thus $\dim(\mathcal{C}^{i.o.}|R(\Delta)) \geq \frac{1}{2}$.

Similarly, $\text{Dim}(\mathcal{C}^{i.o.}|R(\Delta)) < 1$ implies that $\text{Dim}_{\Delta}(f(R(\Delta))) = \text{Dim}(f(R(\Delta))|R(\Delta)) < 1$. By Theorem 4.11 and (4.4), $\text{Dim}(\mathcal{C}^{i.o.}|R(\Delta)) < 1$ then implies that $\dim_{\Delta}(R(\Delta)) < 1$ and thus $\mu_{\Delta}(R(\Delta)) = 0$. Again by the Measure Conservation Theorem, $\text{Dim}(\mathcal{C}^{i.o.}|R(\Delta)) = 1$.

Note that this theorem may also be proven by using a straightforward diagonalization instead of using the Measure Conservation Theorem. \square

Corollary 4.14. *Let \mathcal{C} be a language class that contains the trivial language \emptyset . Then for all $\Delta \supseteq p$, $\dim_{\Delta}(\mathcal{C}^{i.o.}) \geq 1/2$ and $\text{Dim}_{\Delta}(\mathcal{C}^{i.o.}) = 1$.*

Corollary 4.15. *Let \mathcal{C} be a language class that contains the trivial language \emptyset . Then Hausdorff dimension $\dim_H(\mathcal{C}^{i.o.}) \geq 1/2$ and packing dimension $\dim_P(\mathcal{C}^{i.o.}) = 1$.*

Proof. Let Δ be all functions from $\{0, 1\}^* \rightarrow \{0, 1\}^*$. This follows immediately. \square

Now by Observation 3.1 and Corollary 4.6, we obtain (1.5), (1.6) and (1.7) as the following theorem.

Theorem 4.16. *For all $c > 0$*

$$\dim(\text{SIZE}^{i.o.}(n^c) | \text{EXP}) = \dim_{p_2}(\text{SIZE}^{i.o.}(n^c)) = 1/2,$$

$$\dim(P/\text{poly}^{i.o.} | E_3) = \dim_{p_3}(P/\text{poly}^{i.o.}) = 1/2$$

and

$$\text{Dim}(P/\text{poly}^{i.o.} | E_3) = \text{Dim}_{p_3}(P/\text{poly}^{i.o.}) = 1.$$

By Theorem 3.2, the zeroth scale is the best scale for evaluating scaled p_3 -dimension of $P/\text{poly}^{i.o.}$. We cannot obtain more informative strong dimension results about $P/\text{poly}^{i.o.}$ and it is not hard to show that for any infinitely-often class, the scaled strong dimension is 1 for every scale g_i (even for $i < 0$, see [6]). The statement involving strong dimension of infinitely often classes in Theorem 4.13 also generalizes to all scales.

Acknowledgements

I thank Jack Lutz for extremely helpful discussions. I thank John Hitchcock and Elvira Mayordomo for very helpful comments and discussions. I thank anonymous referees for helpful comments. I thank an anonymous referee, Albert Meyer, and Nick Pippenger for bibliographic helps. I also thank Satyadev Nandakumar, Eric Allender, Anumodh Abey, and Fengming Wang for their help in improving the presentation.

References

- [1] E. Allender, When worlds collide: derandomization, lower bounds, and kolmogorov complexity, in: Proc. 21st Annu. Conf. Foundations of Software Technology and Theoretical Computer Science, Lecture Notes in Computer Science, Vol. 2245, Springer, Berlin, 2001, pp. 1–15.
- [2] E. Allender, H. Buhrman, M. Koucký, D. van Melkebeek, D. Ronneburger, Power from random strings, in: Proc. 43rd Ann. IEEE Symp. Foundations of Computer Science, 2002, pp. 669–678, SIAM J. Comput., to appear.
- [3] K. Ambos-Spies, S.A. Terwijn, X. Zheng, Resource bounded randomness and weakly complete problems, Theoret. Comput. Sci. 172 (1–2) (1997) 195–207.
- [4] K.B. Athreya, J.M. Hitchcock, J.H. Lutz, E. Mayordomo, Effective strong dimension, algorithmic information, and computational complexity, SIAM J. Comput., to appear, Preliminary version appeared in Proc. 21st Internat. Symp. Theoretical Aspects of Computer Science, 2004, pp. 632–643.
- [5] F. Hausdorff, Dimension und äusseres Mass, Math. Ann. 79 (1919) 157–179.
- [6] J.M. Hitchcock, J.H. Lutz, E. Mayordomo, Scaled dimension and nonuniform complexity, J. Comput. Syst. Sci. 69 (2) (2004) 97–122.
- [7] J.M. Hitchcock, N.V. Vinodchandran, Dimension, entropy rates, and compression, in: Proc. 19th IEEE Conf. Computational Complexity, 2004, pp. 174–183, J. Comput. Syst. Sci., to appear.
- [8] D.W. Juedes, J.H. Lutz, Weak completeness in E and E_2 , Theoret. Comput. Sci. 143 (1) (1995) 149–158.
- [9] R. Kannan, Circuit-size lower bounds and non-reducibility to sparse sets, Inform. and Control 55 (1982) 40–56.
- [10] J.H. Lutz, Category and measure in complexity classes, SIAM J. Comput. 19 (6) (1990) 1100–1131.
- [11] J.H. Lutz, Almost everywhere high nonuniform complexity, J. Comput. Syst. Sci. 44 (2) (1992) 220–258.
- [12] J.H. Lutz, Dimension in complexity classes, SIAM J. Comput. 32 (2003) 1236–1259.

- [13] J.H. Lutz, The dimensions of individual strings and sequences, *Inform. and Comput.* 187 (2003) 49–79.
- [14] L.A. Sholomov, A sequence of complexly computable functions, *Mate. Zametki* 17 (6) (1975) 957–966 English version, pp. 574–579.
- [15] L. Stockmeyer, The complexity of decision problems in automata theory and logic, Ph.D. Thesis, Massachusetts Institute of Technology, July 1974.
- [16] L.J. Stockmeyer, A.R. Meyer, Cosmological lower bound on the circuit complexity of a small problem in logic, *J. ACM* 49 (6) (2002) 753–784.
- [17] D. Sullivan, Entropy, Hausdorff measures old and new, and limit sets of geometrically finite Kleinian groups, *Acta Math.* 153 (1984) 259–277.
- [18] C. Tricot, Two definitions of fractional dimension, *Math. Proc. Cambridge Philos. Soc.* 91 (1982) 57–74.